Claims

1. A device-to-device authentication system for authenticating whether or not devices on a network are connected within a certain range, characterized in that:

each of said devices interconnected via said network has a mediating device interface for physically accessing a mediating device such that said mediating device is removable, and local environment management means for authenticating that another device physically accessing said same mediating device within a predetermined period of time is located in a local environment where contents are available;

wherein use of said contents is allowed between said devices in said local environment.

2. The device-to-device authentication system according to claim 1, characterized in that:

one of said devices is a home server for legitimately acquiring said contents, whereas the other device is a client for making a request for said contents to said home server for use;

wherein, in response to confirmation of presence of both said devices on said same home network by said local environment management means, said home server provides said contents and/or issues a license for said contents to said client.

3. The device-to-device authentication system according to claim 1, characterized in that:

two or more home servers are able to be installed on said home network;

wherein each said home server provides said contents and/or issues a license for said contents to said client that is confirmed to be present on said same home network.

4. The device-to-device authentication system according to claim 3, characterized in that:

said client is able to be received provision of said contents and/or issuance of said license from two or more said home servers on said same home network.

5. The device-to-device authentication system according to claim 3, characterized in that:

said client is able to use said contents acquired from a plurality of home servers on said same home network, and, upon connection to a home server on an other home network, said client is not able to use said contents acquired from said home servers on said home networks other than said other home network.

6. The device-to-device authentication system according to claim 1, characterized in that:

said mediating device is capable of retaining predetermined identification information; and

said local environment management means authenticates that each of said devices is in said local environment based on a fact that each of said devices physically accessing said mediating device reads the same identification information from said mediating device and/or that time at which each of said devices reads the identification information is within a predetermined period of time.

7. The device-to-device authentication system according to claim 1, characterized in that:

said mediating device has a memory for retaining confidential information in a secure manner;

one of said devices physically accessing said mediating device is capable of generating said confidential information; and

said local environment management means authenticates that each of said devices is located in said local environment based on a fact that said confidential information generated from said one of said devices is able to be acquired by another device via said mediating device within a predetermined period of time.

8. The device-to-device authentication system according to claim 7, characterized in that:

said device generated said confidential information erases said confidential information after elapse of a predetermined period of time; and

said local environment management means authenticates that a device, which is capable of sharing said confidential information prior to loss of said confidential information in said device generated said confidential information, is located in said local environment.

9. A device-to-device authentication method for authenticating whether or not devices on a network are connected within a certain range, characterized in that:

each of said devices interconnected via said network has a mediating device interface for physically accessing a mediating device such that said mediating device is removable; and

said device-to-device authentication method, characterized by comprising:

a local environment management step of authenticating that another device physically accessing said same mediating device within a predetermined period of time is located in a local environment where contents are available; and

a content-using step of allowing use of said contents between said devices in said local environment.

10. The device-to-device authentication method according to claim 9, characterized in that:

one of said devices is a home server for legitimately acquiring said contents, whereas the other device is a client for making a request for said contents to said home server for use;

wherein, in said content-using step, in response to confirmation of presence of both said devices on said same home network, said home server provides said contents and/or issues a license for said contents to said client.

11. The device-to-device authentication method according to claim 9, characterized in that:

two or more home servers are able to be installed on said home network;

wherein, in said content-using step, each said home server provides said contents and/or issues a license for said contents to said client that is confirmed to be present on said same home network.

12. The device-to-device authentication method according to claim 11, characterized in that:

in said content-using step, said client is able to be received provision of said contents and/or issuance of said license from two or more said home servers on said same home network.

13. The device-to-device authentication method according to claim 11, characterized in that:

in said content-using step, said client is able to use said contents acquired from a plurality of home servers on said same home network, and, upon connection to a home server on an other home network, said client is not able to use said contents acquired from said home servers on said home networks other than said other home network.

14. The device-to-device authentication method according to claim 9, characterized in that:

said mediating device is capable of retaining predetermined identification information; and

in said local environment management step, each of said devices is authenticated in said local environment based on a fact that each of said devices physically accessing said mediating device reads the same identification information from said mediating device and/or that time at which each of said devices reads the identification information is within a predetermined period of time.

15. The device-to-device authentication method according to claim 9, characterized in that:

said mediating device has a memory for retaining confidential information in a secure manner;

one of said devices physically accessing said mediating device is capable of generating said confidential information;

and

in said local environment management step, each of said devices is authenticated in said local environment based on a fact that said confidential information generated from said one of said device is able to be acquired by another device via said mediating device within a predetermined period of time.

16. The device-to-device authentication method according to claim 15, characterized in that:

said device generated said confidential information erases said confidential information after elapse of a predetermined period of time; and

in said local environment management step, a device, which is capable of sharing said confidential information prior to loss of said confidential information in said device generated said confidential information, is authenticated that located in said local environment.

17. A communication apparatus for using contents on a network within a predetermined allowable range, characterized by comprising:

a mediating device interface for physically accessing a mediating device such that said mediating device is removable;

local environment management means for authenticating that another device physically accessing said same mediating device within a predetermined period of time is located in a local environment where contents are available; and

content-using means for using said contents legitimately in said local environment.

18. The communication apparatus according to claim 17, characterized in that:

said communication apparatus operates as a home server for providing said contents on said network; and

said content-using means provides said contents and/or issues a license for said contents only to a device confirmed to be present on said same home network by said local environment management means.

19. The communication apparatus according to claim 17, characterized in that:

said communication apparatus operates as a client for making a request for said contents to a home server for use on said network;

said content-using means receives provision of said contents and/or issuance of a license for said contents only from a home server confirmed to be present on said same local environment by said local environment management means.

20. The communication apparatus according to claim 19, characterized in that:

two or more home servers are able to be installed under said local environment;

said content-using means receives provision of said contents and/or issuance of a license for said contents from said two or more home servers confirmed to be present on said same local environment by said local environment management means.

21. The communication apparatus according to claim 19,

characterized in that:

said content-using means is able to use said contents acquired from a plurality of home servers under said same local environment, and, upon connection to a home server on an other home network, said client is not able to use said contents acquired from said home servers under said local environment other than said other home network.

22. The communication apparatus according to claim 17, characterized in that:

said mediating device is capable of retaining predetermined identification information;

said mediating device interface reads said identification information in response to physical access from said mediating device; and

said local environment management means authenticates that a device, which reads the same identification information from said mediating device and/or reads the identification information within a predetermined period of time, is in said local environment of said local environment management means.

23. The communication apparatus according to claim 17, characterized in that:

said mediating device has a memory for retaining confidential information in a secure manner;

said communication apparatus further has a confidential information generation apparatus for generating said confidential information;

said mediating device interface writes said confidential information to said memory of said mediating device in response to physical access from said mediating device; and

said local environment management means authenticates that another devices is located in said local environment of said local environment management means based on a fact that said confidential information generated from said local environment management means is able to be acquired by said another device via said mediating device within a predetermined period of time.

24. The communication apparatus according to claim 23, characterized in that:

said mediating device has a memory for retaining confidential information in a secure manner;

said mediating device interface takes out said confidential information from said memory of said mediating device in response to physical access from said mediating device; and

said local environment management means authenticates that a device, which reads same confidential information from said mediating device and/or reads said confidential information within a predetermined period of time, is located in said local environment of said local environment management means.

25. The communication apparatus according to claim 23, characterized in that:

said confidential information is lost after elapse of a predetermined period of time from generation; and

said local environment management means authenticates that a device, which is capable of sharing said confidential information prior to loss of said confidential information, is located in said local environment.

26. A computer program described in a computer-readable format so as to execute a process, on a computer system, for authenticating whether or not devices on a network are connected within a certain scope, characterized in that:

each of said devices interconnected via said network has a mediating device interface for physically accessing a mediating device such that said mediating device is removable; and

said computer program, characterized by comprising:

a local environment management step of authenticating that another device physically accessing said same mediating device within a predetermined period of time is located in a local environment where contents are available; and

a content-using step of allowing use of said contents between said devices in said local environment.